**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| In re Patent Application of | **MAIL STOP AMENDMENT** |
| Christophe Clavier et al. | Group Art Unit: 2131 |
| Application No.: 09/807,607 | Examiner: Kaveh Abrishamkar |
| Filed: June 1, 2001 | Confirmation No.: 2078 |
| For: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM | |

**REQUEST FOR RECONSIDERATION**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated November 15, 2007, Applicants respectfully request reconsideration of the rejections of the claims. The withdrawal of the previous grounds of rejection is noted with appreciation.

Claims 1-7, 10 and 13-16 were rejected on the grounds of obviousness-type double patenting, in view of the claims of U.S. Patent No. 7,085,378. Without acquiescing in the characterizations of the claims, nor the obviousness of the differences between the claims, as set forth in the Office Action, a Terminal Disclaimer is being submitted herewith, to render moot this ground of rejection.

Claims 13 and 15 were rejected under 35 U.S.C. §102, on the basis of Leppek patent (U.S. 5,933,501), and claims 14 and 16 were rejected under 35 U.S.C. §103, on the basis of the Leppek patent in view of the Kocher et al. patent (U.S. 6,278,783). For the reasons presented hereinafter, it is respectfully submitted that the Leppek patent does not anticipate, nor otherwise suggest, the subject matter

of rejected claims, whether considered by itself or in combination with the Kocher patent.

Claim 13 recites an electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm. The claim recites that the electronic component has a program memory in which is stored a plurality of different manipulating means for producing output data in response to input data. In connection with this claimed subject matter, the Office Action refers to encryption operators 110-1, 110-2, ...110-N described in the Leppek patent as being different manipulating means. As disclosed in the Leppek patent at column 4, lines 14-17, these encryption operators can be conventional encryption algorithms, such as PGP, DES, etc.

Claim 13 further recites that the electronic component includes a processor that executes instructions in the secret key cryptographic algorithm, in accordance with a selected one of the manipulating means. The last element recited in claim 13 is a means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm. In connection with this claimed subject matter, the Office Action refers to the Leppek patent at column 4, lines 33-38. This passage in the patent states:

> [T]he supervisory encryption assembly manager 130 is supplied with an encryption driver or key 170 comprised of a sequence of M access code entries made up of K (at least two and up to all N) address code entries 120 for the encryption operators 110 stored in the database 100.

The Office Action asserts that this key 170 comprises a random value. Applicants respectfully traverse this assertion.

The Leppek patent is not concerned with countermeasures against attacks on secret key cryptographic algorithms. It is directed to the encryption process, per se, and discloses a compound encryption scheme in which a plurality of different types of encryption routines are successively applied to data that is to be encrypted. The successive encryption routines are determined by the sequence of access code entries in the encryption key 170. Referring to the example described in the Leppek patent, beginning at column 5, line 6, each code in the key 170 designates the next successive operator to be employed in the encryption of the data. Referring to column 6, lines 4-14, when the encrypted data reaches the recipient, it is decrypted in accordance with a decryption key 270. This decryption key is the reverse of the sequence in the encryption key.

The decryption key must be known a priori at the recipient, in order for the data to be successfully decrypted. In other words, the data must be decrypted with the encryption operators in the inverse sequence with which it was originally encrypted.

Consequently, the encryption sequence, i.e., the key 170, must be a predetermined value, in order for the decryption to be successful at the recipient end. If the key were a random number, rather than a predetermined value, it would not be known at the recipient, and therefore the recipient would not know the order in which to perform the decryption operations. As such, the key must a predetermined value that is known at both the originating end and the recipient end, in order for the encrypted data to be successfully decrypted. Since the Leppek patent is not concerned with countermeasures, there is no reason to employ a random value to select the codes in the sequence.

Furthermore, the Leppek patent explicitly teaches that the values in the sequence 170 cannot be random. At column 4, lines 49-51, the patent states, with respect to the sequence of code entries 120, that it "is important that the respective codes of any successive pair of codes differ from one another." If the key 170 were truly random, there is no guarantee that this "important" attribute would be achieved. For instance, the patent discloses that the number of code entries in the sequence could be as few as 2. If the sequence values were random, the probability that two successive routines would be the same is as high as the probability that they would be different. Such a result is clearly contrary to the above-quoted teachings of the Leppek patent. Thus, the Leppek patent explicitly teaches away from using a random value to select the encryption operators.

For at least these reasons, therefore, it is respectfully submitted that the Leppek patent does not anticipate the subject matter of claim 13. It employs a predetermined sequence to select the encryption operators that are used to encrypt the data, rather than selecting them on the basis of a random value. The Leppek patent neither discloses, nor otherwise suggests, a random number generator that is employed to select the encryption operators.

Claim 15 recites that the different manipulating means respectively produce sets of output data that are complementary to one another. In rejecting this claim, the Office Action refers to the Leppek patent at column 6, lines 4-14, apparently because it includes the word "complementary". It is respectfully submitted that this portion of the patent does not disclose the subject matter recited in claim 15.

Claim 15 recites that the set of "output data" from one of the manipulating means is complementary to the output data from another one of the manipulating

means. In the context of the rejection, the manipulating means are considered to be the different encryption operators, such as PGP and DES. The patent does not disclose that the output data from these different routines are complementary to one another. Rather, because they are entirely different encryption schemes, their respective sets of output data would be expected to be drastically different from one another, instead of being related to one another, i.e. complementary.

The cited passage at column 6, lines 4-14, does not pertain to the relationship of the output data of different encryption operators. Rather, as discussed previously, this portion of the patent discloses that the sequence of operators employed for decryption is the exact opposite of that which is employed for the encryption. In other words, the encrypted data must be "unwrapped" in the inverse sequence from which it was originally "wrapped". In the patent, the term "complementary" is employed to indicate this inverse sequence. It is respectfully submitted that the Leppek patent does not disclose that the different encryption operators, e.g. PGP, DES, etc., produce outputs that are complementary to one another. Rather, it only discloses that the decryption sequence is the inverse of the encryption sequence.

For this additional reason, therefore, the subject matter of claim 15 is not anticipated by the Leppek patent.

Furthermore, it is respectfully submitted that the Kocher patent, employed in the rejection of claims 14 and 16, does not overcome these differences between the subject matter of the rejected claims and the disclosure of the Leppek patent.

Reconsideration and withdrawal of the rejections, and allowance of all pending claims is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 17, 2008

By: /jamesalabarre/
James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620